The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?

By **Dr. Aysem Diker Vanberg**

Dr. Aysem Diker Vanberg is a Senior Lecturer at Anglia Law School in Chelmsford, United Kingdom. Dr .Diker Vanberg is specialized in IT Law, European Competition Law and Antitrust Law . She may be emailed at *aysem.dikervanberg@anglia.ac.uk.*

H1Abstract

The EU General Data Protection Regulation (GDPR) was published in the Official Journal of the European Union on May 4, 2016.[1] It will become applicable on May 25, 2018. The GDPR provides a new right to data portability for individuals, which requires data controllers to ensure that they can hand over the personal data that has been provided by the data subject himself/herself, in a structured, commonly used and machine readable format, preferably through direct transfer between data controllers.

Following an open public consultation that continued until the end of January 2017, on April 5, 2017, the Article 29 Working Party approved a revised and substantive guidance clarifying some of the ambiguities with regards to the right to data portability.[2]

This article examines the development of the right to data portability in the European Union and seeks to draw lessons from the European experience with a view to make suggestions particularly for the United States and other jurisdictions. It concludes that the GDPR, both as legislation and as an agile legislative process, will offer valuable insights to other jurisdictions once they recognize the need for individual data portability rights. Further research particularly into enforcement issues as well as the economics of the right to data portability is suggested, as well as research into what the European Union can learn from the United States.

H1**Introduction**[3]

On January 25, 2012, the European Commission (the Commission) proposed a reform of the EU's data protection rules by drafting the General Data Protection Regulation (GDPR) in order to strengthen online data protection rights and boost Europe's digital economy. It was also done to adapt to technological advancements that had taken place in the previous decade, following the introduction of the Data Protection Directive.[4] While the provisions of the GDPR build upon those established under the Data Protection Directive, the rules under the GDPR are more stringent[5] and hold a wider scope.[6] The reactions to the GDPR have been mixed. Some scholars[7] saw it as a welcome development, however others[8] have raised concerns.

The right to data portability in the GDPR will require businesses to ensure that they can hand over personal data provided by an individual[9] in a usable and transferable format. The preamble of the GDPR demonstrates that the right to data portability will be applicable to cloud computing, Web services, smartphone systems and other automated data processing systems.[10] The right to data portability will apply to a wide range of areas such as social media, search engines, photo storage, email and online shops. It will be equally applicable to banks, pharmaceutical companies, energy providers, airlines—even small businesses such as pizza shops or tailors if they are data controllers and deal with personal data.

The final text of the GDPR was agreed to in the trilogue between the European Council, Parliament and Commission on December 15, 2015, and published on May 4, 2016 in the Official Journal of the European Union.[11] After a two-year transition period, the GDPR will be binding on all member states from May 25, 2018.

The right to data portability is contained under Article 20 of the GDPR. It can be seen as an extension of an individual's right of access under Article 15 of the GDPR.[12] It has two

key elements: (1) the right of the data subject to obtain a copy of personal data from the data controller; and (2) the right to transfer that data from one data controller to another. The text of the GDPR arguably limits the scope of the right to data portability and contained some ambiguities. Following an open public consultation, which ran through the end of January 2017, on April 5, 2017, the Article 29 Working Party[13] approved a revised and substantive guidance (hereinafter referred to as the 2017 revised guidelines on data portability) clarifying some of the ambiguities with regards to the right to data portability.[14]

This article examines the right to data portability under the GDPR to establish whether any lessons can be drawn from the EU experience, particularly for the United States. This article critically analyzes the issues raised by Article 20 of the GDPR and potential enforcement problems. It also gives an overview of the state of data portability in the United States and provides lessons to be learned from the EU experience.

H1Critical Review of the Right to Data Portability—Key Issues in the GDPR[15]

H2Limitations on Data Generated by the Data Controller

Article 20 of the GDPR only applies to data provided by the data subject. The Article 29 Working Party published a summary of discussions that took place at the Fablab Workshop July 26, 2016.[16] It gave a good overview of key issues in relation to data portability.

In the context of data portability, Article 29 Working Party highlighted the importance of clarifying what is meant by data that has been provided by the data subject, as a narrow interpretation of personal data would result in fewer benefits for individuals while a very wide interpretation of it would be a concern for data controllers.[17]

As mentioned by Graef et al, the wording of Article 20 of the GDPR does not clarify whether the data that has been generated by the service provider for statistical and analytical purposes, such as online reputations, could be subject to data portability or not.[18]

As pointed out by Graef et al,[19] in an auction Web site such as eBay the contact information and the advertisements are provided by the seller (data subject) himself but the provider adds feedback scores to the seller's profile and these form part of the reputation that a seller has built on. Hence, a literal interpretation of the adopted text would only allow the users to move their personal information to another auction site while not being able to move their ratings and reputation to another auction site as the latter is provided by the service provider. For an online user it is crucial to show that he/she has built a good reputation when he/she moves on to a different platform. Without moving this reputation, it is highly unlikely that the seller would attract new buyers in a new platform. Ultimately, this can hinder users from moving to another platform.

The April 2017 revised guidelines on the right to data portability offer some helpful clarification with regards to the above-mentioned ambiguity by stipulating that data provided by the individual should include "the personal data that are observed from the activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of Web site usage or search activities."[20] In other words, according to the revised guidelines on the right to data portability the term provided by data subject includes the data that result from the observation of an individuals' behavior but it does not cover 'inferred' data resulting from the subsequent analysis of that behavior by the data controller.[21] Hence it could be said that Article 29 Working Party takes a broader interpretation of personal data, which is a welcome interpretation in terms of extending the scope of data portability in the EU member states.

In the context of Graeff's example, buyer/seller ratings on eBay would fall within the scope of observed data, which would be portable from one controller to another, while an average of these scores calculated by the data controller (processor), would not.

The Article 29 Working Party also clarifies that meta data that is needed to meet the data subjects' objective, to move data from one service to another, falls within the scope of Article 20 of the GDPR.[22] As an example, the right to data portability would require a data controller to not only transfer the emails sent and received by the data subject but also other relevant information such as timestamp information and other information showing whether emails have been read or not.

The clarifications in the revised guidelines on data portability go a long way in meeting the need for clarification. Nevertheless, it will be interesting to see whether data controllers will find ways of circumventing the revised guidelines in order to refuse to transfer data to another controller and it will be important to monitor any potential problems in order to address them in the future.

H2 Privacy Rights of Third Parties

Another limitation of the right to data portability concerns the privacy rights of third parties. As noted by Engels, allowing one user to transfer a second user's information to another platform may violate the privacy rights of a second user.[23] For example, when several people appear in a photograph on Facebook, even if one data subject wants to import it to another social networking platform, this cannot be done, as it would impact privacy and data portability rights of other individuals appearing in that picture. Another example is a bank transfer with information pertaining to both buyer and seller. This implication seems to have been taken into account by the legislators as paragraph 4 of Article 20 GDPR states that the right to data shall not adversely affect the rights and freedoms of others.

The revised guidelines by the Article 29 Working Party make it clear that even if the requested data might have an impact on the privacy rights of third parties this does not stop it from being transferred to another controller.

Their proposed solution to deal with potential shortcomings is two–pronged. First, "The processing operations initiated by the data subject in the context of personal activity that concern and potentially impact third parties remain under his or her responsibility, to the extent that such processing is not, in any manner, decided by the data controller."[24] In other words, according to the April 2017 Guidelines on the right to data portability, if the data relates to the person making the request as well as third parties, it is the responsibility of the person making the request to ensure that data protection right of third parties are respected.

Second, the revised guidance asserts that "the rights and freedoms of third parties will not be respected if the new data controller uses their personal data for purposes other than to deliver a service to the data subject who has ported the data.[25]" For instance, if the new data controller uses the data of third parties for direct marketing purposes, it would be contrary to the revised guidelines on data portability.

H2Technical Feasibility of Data Transfer

A significant challenge for the enforcement of the right to data portability concerns the "technical feasibility" sought for the data portability across the platforms. Arguably, what is technically feasible for one data controller might not be technically feasible for another data controller. Given the wording of Article 20(2) of the GDPR it is likely that some data controllers will contend that such a transfer is technically infeasible. As a result of this wording the transfer of data may be undermined and overlooked by data controllers. As there is no reference to the Commission's authority to specify the electronic format necessary for data portability in the GDPR, collaboration among market players is crucial in devising industry norms and standards.

In its revised guidelines issued on April 2017, the Article 29 Working Party offers valuable clarification with regards to the notion of technical feasibility and controller to controller transfer.

Article 29 Working Party states that "where no formats are in common use for a given industry or given context, data controllers should provide personal data using commonly used open formats (*e.g.*, XML, JSON, CSV) along with useful metadata at the best possible level of granularity**,** while maintaining a high level of abstraction."[26]

As regards "technically feasible" Article 29 Working Party holds that "… direct transmission from one data controller to another could … occur when communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data."[27] This can be interpreted as there being no impediment to invest in new functionality where existing systems do not support controller-to-controller transfer.

In terms of enforcing direct controller-to-controller portability it seems that the Article 29 Working Party has chosen to rely on two mechanisms to motivate direct transfer: (1) data subject pressure by empowering data subjects to demand an explanation as to why data controllers are unable to offer direct controller-to-controller portability;[28] and (2) the administrative burden of repetitive data subject requests, where data subjects can be expected to demand usable data vis-à-vis a range of disparate systems.[29]

Whether the pressure from data subjects to ensure direct controller-to-controller portability will prove effective, remains to be seen. It will be interesting to see whether data controllers will come up with ways to circumvent data portability by suggesting that such transfer is not technically feasible, when it is in fact possible.

A stricter requirement for direct controller-to-controller transfer could still turn out to be a necessity, one that in a few years with open Web technologies will seem both more reasonable and more feasible.

H2Disproportionate Costs and Efforts

Forcing data controllers to transfer personal data may result in disproportionate costs and efforts.

Article 20 of the GDPR requires an online service to write specialized code—export-import module (EIM)—that will export data from that service and import it to another service. As noted by Swire and Lagos, many small and medium-sized companies do not have the resources to fully understand the GDPR, comply with it and write an EIM to move data to another provider.[30]

Neither the Commission nor other EU institutions have presented any figures as to the cost of complying with data portability requests. According to a study by Christensen *et al*, the GDPR reform would increase European small and medium-sized enterprises' annual IT costs by between approximately € 3.000 and € 7.200 depending on the industry the particular SME is operating in, representing between 16 and 40 percent of their yearly average IT budgets.[31] It is not clear what percentage of this budget will be spent responding to data portability requests.

Swire and Lagos also support this point and argue that the GDPR would impose substantial costs on suppliers of software and apps.[32]

While such costs may not be significant for large companies, the requirement is likely to create problems for small and medium-sized companies. It must be noted that complying with the GDPR should not to be taken lightly due to the heavy fines associated with failing to do so. According to Article 83(5) of the GDPR, a data controller that fails to comply with data portability provisions in the GDPR will incur administrative fines up to 20 million EUR or in case of an undertaking up to 4 percent of the total worldwide annual turnover of the preceding year, whichever is greater.

The issue of disproportionate costs also was raised in December 2015 by Baroness Neville Rolfe, the United Kingdom's parliamentary Under-Secretary of State for the Department for Business, Innovation and Skills. She stated that data portability rules designed to enable consumers to move their data from one platform to another should not be too costly as they can serve as an entry barrier into markets, and this might have an adverse effect on innovation and competition.[33]

The Article 29 Working Party, however, does make it clear in the guidelines that the role of being data controller in the European Union moving forward should be considered a normal cost of doing business along the lines of accounting, insurance, and other unavoidable costs. The Article 29 Working Party explicitly holds that the overall system implementation costs cannot "be used to justify a refusal to answer portability requests."[34] Time will show whether dealing with data portability requests will be too costly for businesses or whether these costs could be seen as an ordinary cost of running a business as suggested by the Working Party.

H2Proprietary information and intellectual property rights

If the personal data that needs to be transferred contains valuable proprietary information and intellectual property, this might discourage companies/service providers from creating the proprietary information in the first place.

The case of True Fit,[35] an online digital service helping users of online clothing retailers such as House of Fraser to find the right cloth sizes for their shoppers, illustrates this point. The True Fit service asks shoppers to share a wide range of personal data such as height, weight, measurements, body type, and information such as what brand and size their favorite clothing comes from. Users share this information with True Fit, which then shares it with online retailers. Arguably, if True Fit were to be required under the data portability provision to transfer this data to other retailers, its business model would become obsolete.

Recital 63 of the GDPR provides that the general right of access under Article 15 could be restricted if it adversely affects the rights and freedoms of others, including trade secrets and intellectual property rights. As the right to data portability can be seen as an extension of the right of access, arguably the limitation mentioned in Recital 63 should be applicable in the context of data portability requests. In other words, when faced with data portability requests companies, data controllers should be able to strip valuable data from the dataset if it adversely affects trade secrets and intellectual property.

Nevertheless, neither recital 68 of the GDPR pertaining to the limitations of the right to data portability, nor Article 20 of the GDPR specifically suggests that the right to data portability can be limited if it adversely affects trade secrets and intellectual property. Hence there was a need for further clarification as to whether the right to data portability might be restricted when it affects proprietary information and intellectual property rights.

If companies, such as True Fit, stop creating valuable services based on personal data, clearly this will have a stifling effect on innovation and consumer welfare. This would, ultimately, have an adverse effect on consumers who would be deprived of choice and useful products.

In the revised guidelines on the right to data portability, the Article 29 Working Party provides some guidance with respect to the above and holds that "The right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights."[36] Furthermore in its guidance the Article 29 Working Party suggests that data controllers can provide the information requested in a form that does not release information covered by trade secrets and intellectual property rights.[37] However it must be noted that this might not be always easy to implement. Hence there is definitely need for further guidance on this issue.

As seen above in the discussion of privacy rights of third parties, the Article 29 Working Party guidelines on data portability fail to offer protections for current data controllers, while making it clear that the data subject, and the receiving data controller has every right to request data when the purpose is to provide a service to the data subject, regardless of the impact on the current data controller.

In light of the above, it is unclear whether a third party data controller such as True Fit will be able to stop competitors, or current customers, from receiving information and use their service for free. Time will show if such firms and services will potentially suffer due to business models seemingly at odds with the GDPR, and what the cost of that will be to consumers and to the economy.

H2Enforcement Issues Pertaining to the Right to Data Portability

The main objective of the right to data portability is to empower consumers so that they can get a copy of their electronic personal data, demand transmission of their personal data to another provider and switch to other providers.[38] Hence, the objective of the right to data portability overlaps with the objectives of other areas of law, *e.g.*, competition law, consumer protection laws, and so forth.

Similar to other data subject rights in the GDPR, data portability is a right, which needs to be invoked by the data subject and cannot be relied on by parties such as small and medium sized businesses. For instance, a small business cannot demand data portability from its business bank but an individual can. This raises some problems regarding its legal and theoretical boundaries, as well as enforcement within the realm enshrined by the GDPR.

Furthermore, there is no clarity as to whether users will make use of the right to data portability. In order to ensure that data subjects invoke the right effectively, data subjects need to be informed as to what this right entails.

Hence, Article 29 Working Party should liaise with national data protection agencies in order to make sure the necessary investments are made in educating the public about their rights. As a minimum, national data protection agencies should have information on their Web sites in plain and simple language explaining to users how they can approach the data controller for data portability requests and advise them on how to make a complaint if the data controller refuses to provide the data. Making a complaint must be easy and the data subjects should not incur substantial costs or risks as this might discourage them from exercising their rights.

Furthermore, while the Article 29 Working Party guidelines do not refer to enhancing competition between services as an objective of data portability, several authors[39] have suggested that competition law and provisions may contribute to the enforcement of data portability legislation, in particular where the data controller is a dominant actor in a monopolistic market applying unfair restrictions on data portability. In this context, failure to offer direct controller-to-controller data portability without a valid and sensible reason could be seen as an abuse of a dominant position (or monopolization in the US context) and potentially be remedied by competition/antitrust laws.

H2Privacy and Data Security Risks

Security and privacy concerns arise when data is transferred from one data controller to another. Data can end up in the wrong hands if access is granted to the wrong person—an investigator making a pretext call, a conman engaged in identity theft, a hacker, or, in some instances, one family member in conflict with another.[40] Ironically, interoperable solutions as suggested in the GDPR[41] could aggravate security concerns at the expense of uniform rules and processes in this context. Although not seen as the main cause of the security vulnerabilities, interoperability is regarded as one of the factors that increase the number of opportunities for security breaches and the potential fall-out from such breaches.[42]

Particularly for small and medium sized businesses (SME) with limited resources to invest in data security, this is a significant concern.

The Article 29 Working Party arguably has not succeeded in offering more clarity as to what security standards are expected. It places the responsibility for data security squarely on the current data controller, and suggests that risk mitigation measures may include "using additional authentication information, such as a shared secret, or another factor of authentication, such as a onetime password; suspending or freezing the transmission if there is suspicion that the account has been compromised; in cases of a direct transmission from a data controller to another data controller, authentication by mandate, such as token-based authentications, should be used." [43]

It can be argued that more detailed guidance should be offered, in particular as regards the extent of responsibility and mandate a data controller has in assessing the security of the receiving controller and the ability of the data subject to keep the requested data secure. While 20 years of financial records can be reasonably expected to be safe when controlled by a bank, they are likely to be a lot less safe if downloaded as a spread sheet to an unprotected smartphone.

There are situations arguably where a data controller should have the right to refuse data portability due to concerns about security at the receiving end, hereunder uncertainty about the identity of the recipient and uncertainty surrounding the receiving data controller's ability to protect personal and third party data.

H1Data Portability in the United States

Data portability has been a contentious issue in the United States as well. The United States does not have a uniform data protection law similar to the European Union and there is no single regulatory authority dedicated to overseeing data protection law in the United States. Concerning the right to access data collected by companies the United States relies on a

patchwork of state and sector specific federal laws for credit agencies and data brokers.[44] Furthermore, there are many guidelines, developed by governmental agencies and industry groups that are part of self-regulatory guidelines and frameworks that are considered "best practices, which are not legally binding.[45]

In the United States, the Federal Trade Commission is the federal privacy regulator regarding consumer protection, which also is relevant for the online environment.

Needles to say in the United States there is not a single provision that deals with the right to data portability, which is comparable to the European Union. In the United States, data portability generally is seen as an access to information/data issue.

The 1996 Health Insurance Portability and Accountability Act (HIIPA) is the first and most wide ranging data portability initiative giving individuals the right to access personal health information collected about them,[46] delivered, *e.g.*, on a storage device such as a USB drive. While offering the right to access data HIPAA does not currently address the need for controller–to–controller data portability.

In 2010, former US President Obama launched a series of initiatives entitled “My Data initiatives” to ensure that US citizens has easy and secure access to their own personal data.[47]

My Data Initiatives required the US Government to work together with the Federal Government, public and private sector to facilitate US citizens’ access to their own personal data in a variety of sectors. As an example, Blue Button,[48] a data healthcare initiative, aimed to expand patients’ access to their medical records so that data subjects can track their own health records and health information, which also can be shared with doctors and specialists[49].

The Green Button[50] initiative allowed US citizens to access their detailed household or building electricity records in order to facilitate virtual energy audits with a view to identify inefficiencies and save money by switching providers.[51]

My Transcript[52] initiative allows data portability for the Internal Revenue Service and finally My Student[53] Data initiative allows US students to download information in relation to federal student grants and or loan information.

As pointed out by Macgillivray and Shambraugh, many private service providers have embraced data portability but there are still many other areas where data portability has not been required under US law and is not available in particular.[54]

On September 30, 2016, the Office of Science and Technology Policy (OSTP) asked various stakeholders their thoughts on the potential benefits and drawbacks of increased data portability, the industries that would most benefit and be harmed by increased data portability, the specific steps the Federal Government and private companies and others might adopt to encourage greater data portability and the best practices in implementing data portability.[55]

OSTP received 23 comments from several stakeholders including companies, trade associations, advocacy groups, and individuals.[56] Roughly half of the commentators limited their comments to health data and data portability pertaining to it. Many commenters praised the potential benefits of data portability for users. The respondents suggested that an increased data portability would improve financial awareness, increase user exploration of new services, ease the burden of backing up data, increase user control and user trust and lower barriers to entry for services.[57] Some commentators raised concerns as to the cost of data portability and the increasing complexity of data portability between services due to the lack of commonly agreed standards.

Furthermore, some respondents suggested that data portability requirements might raise barriers to entry if they prove too be too burdensome to implement. One commentator summed up the views of several other commentators by stating that "portability should be incentivized but not mandated."[58] Some commentators suggested that mandatory data portability rules would be inefficient, ineffective and be premature for rapidly developing

industries and this might have a negative impact on innovation.[59] Finally,respondents suggested that the government could incentivize data portability by increasing consumer awareness of it, leading by example or through encouraging interoperability and open standards, which would create the right environment for data portability.[60]

As data continues to increase in value both to users and service providers, ensuring data portability will become ever more crucial. From the above consultation, it is clear that data portability is quite desirable in the United States as well. Nevertheless based on the answers of the respondents it might be said that having a mandatory rule that applies across all sectors, is not very desirable for the industry stakeholders. Sarah Holland from Google illustrates this point and states that "one size fits all" requirements in relation to data portability may promote consistency but it is an ineffective approach, as it might create artificial barriers to new services entering the market place.[61] Arguably the right to data portability in the European Union and its successful implementation could prove useful in alleviating the concerns of the industry players.

The OSTP consultation and the responses obtained from various stakeholders provide very useful insights in relation to data portability in the US context. Nevertheless, it is worth noting that the OSTP consultation received only 23 responses and the majority of the responses were obtained from industry players and associations. This shows that there is a need for a more extensive consultation and debate in the United States, which takes into account the views of diverse stakeholders particularly consumers to have a more nuanced and more insightful review of the right to data portability.

H1Conclusion—What Lessons Can Be Drawn from the EU Experience

The objective of this article was to examine development of the right to data portability in the European Union under the GDPR with a view to establish whether any lessons can be drawn from the EU experience particularly for the United States.

As with the exception of sector specific regulation for the Health Sector (HIPAA) and voluntary programs, there is as of yet no such thing as data portability provision in the United States comparable to Article 20 of the GDPR. Hence a side-by-side comparison between the European Union and the United States is not relevant.

The GDPR is unprecedented in geographical reach and in scope, far surpassing any equivalent legislation anywhere in the world. The European Union currently is in uncharted territory as it sets out to break new ground in the area of data governance and in particular in the context of data portability rights for individuals. As such the European Union can offer the United States and other jurisdictions a wealth of insight as it explores ways of driving data portability across sectors.

First, the United States operates under the assumption that data portability is a choice for data controllers, not a right for data subjects. As such, much of the insight offered by the development of right to data portability under the GDPR has little relevance until the United States decides to see data portability as a fundamental right for data subjects. While the above-mentioned My Data Initiatives are commendable and certainly have driven innovation (although with limited adoption) in specific industries, they only apply to those industrial actors who see moral and economic sense in data portability and there is no penalty for not complying with these initiatives. In this regard, the first thing the United States can take away from the data portability legislation in the GDPR may be as simple as: In the near future some form of legislation that comprises a right to data portability at federal level which applies to all industries and all firms, not just to a select few, is required. Such legislation does not need to be as rigid as the GDPR and can be shaped by taking into account the views of all relevant stakeholders including industry players and consumers.

Second, if and when the United States eventually decides to catch up and adopt data protection legislation, which includes a right to data portability they will benefit from second

mover advantage, being able to walk in the steps of the European Union where advantageous, while avoiding known pitfalls. The GDPR is far from being perfect and arguably still a work in progress however the United States and other jurisdictions definitely will benefit from following the European discourse with regards to the definition of data observed by the data subject, the privacy rights of third parties, the possible need for enforcement pertaining to direct transfers between data controllers, the treatment of proprietary information and intellectual property rights, privacy and data security risks in transferring information in order to draw lessons.

Third, the United States probably will benefit from observing the agile process with which the GDPR, and maybe Article 20 in particular, has seen the light of day. The GDPR deals with new technological realities in fast moving markets. To expect perfection from the GDPR would be unrealistic. The combination of the GDPR combined with guidelines seems to be working very well in this context, offering a reasonably high degree of predictability in an emergent environment.

As the article demonstrates, the United States barely has started addressing data portability; nevertheless US firms will have to comply with the requirements of the GDPR in the European Union as of May 2018. While the main purpose of the GDPR is to give EU citizens control over their personal data, it has an extra territorial reach. The GDPR applies to any company that operates in the European Union. Hence a large amount of US businesses including Google, Facebook, Microsoft that collect data from EU data subjects need to comply with the GDPR to avoid hefty fines. In this respect, it is likely that the United States will soon have to engage with the need for convergence in global data protection and more specifically data portability policy.

For the European Union and the United States, important research themes are emerging. In the context of this article, three themes stand out.

First, in order to ensure successful enforcement of data portability there is a need to monitor and analyze the reasons offered by data controllers for refusal to comply with data portability requests, in particular relating to direct transfer between data controllers. This way, future guidelines can be adopted to address issues that hinder controller to controller data portability.

Second, interdisciplinary research is needed to ascertain the economic effects of data portability under the GDPR. As mentioned by several commentators,[62] personal data is the new oil. Hence legislating how an individual's personal data should be made available to other parties has wide ranging consequences and such legislation should be treated very cautiously. It is important to ascertain to what degree the data portability provision under Article 20 of the GDPR drives innovation, economic growth and consumer welfare, delivering on the promise of the European Digital Economy.

Finally, it is inspiring to see the results achieved by the US My Data initiatives such as Green Button. In this respect, the European Union would clearly benefit from research into what the United States gets right, in particular with reference to driving innovation and economic growth through constructive and transparent engagement with industry.

NOTES

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.
[2] Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01 adopted on April 5, 2017.
[3] This introduction borrows extensively from the author's earlier article on the right to data portability, *see* Aysem Diker Vanberg & Mehmet Bilal Unver, "The Right to data portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?" *European Journal of Law and Technology*, 8(1) (2017).
[4] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data OJ L 281/31 (1995).
[5] Sarah Downey, "The Most stringent data laws in the world: European Union agrees on penalties to protect personal data," *Legal Business*, December 16, 2015,

https://www.legalbusiness.co.uk/blogs/the-most-stringent-data-laws-in-the-world-european-union-agrees-on-penalties-to-protect-personal-data, accessed December 18, 2017.

[6] Rhys Hadden, "The EU General data protection regulation: The new data protection landscape," *Guildhall Chambers*, May 2016, accessed December 18, 2017.

[7] See for instance, Alexander Brown and Clare Adam, "The draft regulation–does every cloud have a silver lining?," 12(4) *P& DP* 9 (2012); Winston J. Maxwell, "Data Privacy: the European Commission pushes for total harmonisation," 18(6) *CTLR* 175 (2012).

[8] See for instance, Nick Graham, "Data protection and privacy," 98 (Aug) *COB* 1 (2012); Sana Khan, "Practitioner's insight into the new EU Data Regulation," 5(1) *Comp& Risk* 6 (2016); Eduardo Ustaran, "EU General Data Protection Regulation: things you should know," 16(3) *P & DP* 3 (2016); Anita Bapat, "The new right to data portability," 13(3) *P & DP* 3 (2013); Francoise Gilbert, "European data protection 2.0: new compliance requirements in sight—what the proposed EU data regulation means for US companies," 28(4) *Santa Clara High Technology Law Journal* 815 (2001).

[9] In this article the terms "individual," "consumer," "user," and "data subject" are used interchangeably to refer to a "data subject." According to Article 4 of the GDPR a "data subject" is an identifiable natural who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[10] Gabriela Zanfir, "The Right to Data Portability in the Context of Data Protection Reform," 2(3) *International Data Privacy Law* 149 (2012).

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.

[12] Bapat, *supra* n.8.

[13] The "Article 29 Working Party" is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC on data protection. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonized policies for data protection in the EU Member States.

[14] Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01 adopted on April 5, 2017 (hereinafter referred to as revised Guidelines on the right to data portability)

[15] This section of the article borrows from the author's earlier article on the right to data portability, *see* Aysem Diker Vanberg & Mehmet Bilal Unver, "The Right to data portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?," *European Journal of Law and Technology*, 8(1) (2017).

[16] Fablab Workshop is a workshop organized by the Article 29 Working Party in Brussels on July 26, 2016, with more than 90 participants including 40 representatives from Data protection Authorities. Among other issues the participants have discussed the issues relating to data portability. *See* Fablab, "GDPR/from concepts to operational toolbox, DIY," Results of the discussion (2016) available at *http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2016/20160930_fablab_results_of_discussions_en.pdf*, accessed December 18, 2017.

[17] Fablab, *supra* n.16.

[18] Inge Graef, Jeroen Verschaleken, Peggy Valcke, "Putting the right to data portability into a competition law perspective," *Law: The Journal of the Higher School of Economics, Annual*

Review 4 (2013), available at SSRN: *http://ssrn.com/abstract=2416537*, accessed December 18, 2017.
[19] *Id*.
[20] Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, pages 9-10.
[21] *Id*. at 10.
[22] *Id*. at 11.
[23] Barbara Engels, "Data portability amongst online platforms," 5(2) *Internet Policy Review* 4 (2016) at *http://policyreview.info/articles/analysis/data-portability-among-online-platforms*, accesed December 18, 2017.
[24] Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, at 11.
[25] *Id*. at 11- 12.
[26] *Id*. at 18.
[27] *Id*. at 16.
[28] *Id*. at 16.
[29] *Id*. at 15.
[30] Peter Swire and Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," 72 *Maryland Law Review* 335 (2013).
[31] Laurits R Christensen, Andrea Colciago, Federico Etro, Greg Rafaert, "The Impact of the Data Protection Regulation in the EU," *European Financial Review* 72 (2013).
[32] Swire and Lagos, *supra* n.30 at 379.
[33]John Bowman, "New UK Minister's Data Protection To-Do List," (2015), *https://iapp.org/news/a/new-uk-ministers-data-protection-to-do-list/*, accessed December 18, 2017.
[34] Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, at 15.
[35] True Fit is footwear and apparel's discovery platform, which uses personal data obtained from users to enable them to find a better fit for clothing and footwear. The information on True Fit is available at *truefit.com,* accessed November 17, 2016.
[36] Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, at 12.
[37] *Id*.
[38] Bapat, *supra* n.8 at 4.
[39] *See* for instance Vanberg & Unver, *supra* n.3; *see also* Graef, Verschaleken, and Valcke, *supra* n.18.
[40] Final report of the Federal Trade Commission Advisory Committee on Online Access and Security 19-25
(May 15, 2000), *https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf*, accessed December 18,, 2017; *see also* Swire and Lagos, *supra* n.30 at 374.
[41] The GDPR, Recital 68.
[42] Urs Gasser, "Interoperability in the digital ecosystem," Berkman Center Research Publication No. 2015-13 12 (2015), available at *SSRN http://ssrn.com/abstract=2639210* accessed December 18, 2017.
[43] Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, at 19.

[44] Samuel Grogan and Aleecia M. McDonald "Access Denied! Contrasting Data Access in the United States and Ireland," Proceedings on Privacy Enhancing Technologies (3) 192 (2016).
[45] "Data Protection in the United States," Thomson Reuters Practical Law at *https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1* accessed December 18, 2017.
[46] Grogan and McDonald, *supra* n.44.
[47] Kristen Honey, Phaedra Chrousos, and Tom Black, "My Data: Empowering All Americans with Personal Data Access," *https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access*, accessed December 18,, 2017.
[48] More information on Blue Data initiative can be found online, *https://www.healthit.gov/patients-families/your-health-data*, accessed December 18,, 2017.
[49] Honey, Chrousos, and Black, *supra* n.47.
[50] More information on Green Button initiative can be found online, *https://energy.gov/data/green-button*, accessed December 18,, 2017.
[51] Honey, Chrousos, and Black, *supra* n.47.
[52] More information on My Transcript initiative can be found online, *https://www.irs.gov/individuals/get-transcript*, accessed December 18,, 2017.
[53] More information on my student data information is available at *https://studentaid.ed.gov/sa/resources/mystudentdata-download*.
[54] Alexander Macgillivray and Jay Shambaugh, "Exploring data portability, The White House Archives, *https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability*, accessed December 18, 2017.
[55] *Id*.
[56] *Id*.
[57] White House Office of Science and Technology Policy Request for Information regarding data portability Public Responses (January 10, 2017), *https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/OSTP-Data%20Portability-RFI-Responses_for_humans.pdf*, accessed December 18,, 2017.
[58] *Id*.; *see* respondent Jordan Gross, U.S. Chamber Technology Engagement Center, pp. 29.
[59] White House Office of Science and Technology Policy Request for Information regarding data portability Public Responses, *supra* n.57. On this point see the respondent Sarah Holland, Google at page 32.
[60] *Id*.
[61] *Id*.
[62] *See* for instance, Meglena Kuneva, "Roundtable on Online Data Collection, Targeting and Profiling," SPEECH/09/156, *http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm*, accessed December 18, 2017.